STATEMENT OF LARRY D. JOHNSON

Special Agent in Charge
Criminal Investigative Division
United States Secret Service

Before the Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census

U.S. House of Representatives

September 22, 2004

Good afternoon, Mr. Chairman. I would like to thank you, as well as the distinguished Ranking Member, Mr. Clay, and the other members of the subcommittee for providing an opportunity to discuss the subject of information security, and the role of the Secret Service in safeguarding our financial and critical infrastructures.

In addition to providing the highest level of physical protection to our nation's leaders, the Secret Service exercises broad investigative jurisdiction over a wide variety of financial crimes. As the original guardian of our Nation's financial payment systems, the Secret Service has a long history of protecting American consumers and industry from financial fraud. For two decades, the Secret Service has been the primary federal law enforcement agency responsible for the investigation of access device fraud, including credit and debit card fraud. In addition, we have concurrent authority with other law enforcement agencies in identity crime cases. In recent years, the combination of the information revolution, the effects of globalization and the rise of international terrorism has caused the investigative mission of the Secret Service to evolve dramatically. The explosive growth of high tech and international crimes has led the Secret Service to become an agency that is recognized worldwide for its expertise in the investigation of all types of financial crimes. Our efforts to detect, investigate and prevent financial crimes are aggressive, innovative and comprehensive.

After 138 years in the Treasury Department, the Secret Service was transferred last year to the Department of Homeland Security with all of its personnel, resources and investigative jurisdictions intact. Today, those responsibilities require us to be involved in the investigation of traditional financial crimes as well as identity crimes and a wide range of electronic and high-tech crimes.

The burgeoning use of the Internet and advanced technology, coupled with increased investment and expansion, has intensified competition within the financial sector. While these advances have produced a number of benefits to consumers, we must also recognize that with lower costs of information-processing, legitimate companies have found it profitable to specialize in data mining, data warehousing and information brokering. Information collection has become a common byproduct of newly-emerging e-commerce. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by businesses seeking to find the best customers for their products. This has led to a new measure of growth within the direct marketing industry that promotes the buying and selling of personal information.

In today's markets, consumers routinely provide personal and financial identifiers to companies engaged in business on the Internet. They may not realize that the information they provide in credit card or loan applications, or to merchants they patronize is a valuable commodity in this new age of information trading. Consumers may be even less aware of the illegitimate uses to which this information can be put. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders. But legitimate business can provide a first line of defense against identity crime by safeguarding the information it collects. Such efforts can significantly limit the opportunities for identity crime, even while not eliminating its occurrence altogether.

Identity crime is the theft or misuse of an individual's personal or financial identifiers in order to gain something of value or to facilitate other criminal activity. Types of identity crime include identity theft, credit card fraud, bank fraud, check fraud, false identification fraud and passport/visa fraud. It is equally important to note that identity crimes are used to facilitate and fund other serious crimes such as narcotics and weapons trafficking, organized crime, mail theft and fraud, money laundering, immigration fraud and terrorism. Identity crimes provide the anonymity for criminals to operate undetected and untraceable financing to fund their criminal endeavors.

According to statistics compiled by the Federal Trade Commission for 2003, 42% of the 516,740 victim fraud complaints reported involved at least one type of identity crime. The complaints were broken down as follows *(note that some complaints involved more than one of the listed activities):*

- **33%** of complaints involved credit card fraud – i.e. someone either opened up a credit card account in the victim's name or "took over" his or her existing credit card account;

- **21%** of complaints involved the activation of telephone, cellular, or other utility service in the victim's name;

- **17%** of complaints involved bank accounts opened in the victim's name, and/or fraudulent checks negotiated in the victim's name;

- **11%** of complaints involved employment-related fraud;

- **8%** of complaints involved government documents/benefits fraud;

- **6%** of complaints involved consumer loans or mortgages that were obtained in the victim's name; and

- **19%** of complaints involved some type of miscellaneous fraud, such as medical, bankruptcy and securities fraud.

Although financial crimes are often referred to as "white collar", this characterization can be misleading. The perpetrators of such crimes are increasingly diverse, and today include both domestic and international organized criminal groups, street gangs, convicted felons and terrorists.

These criminals seek the personal identifiers generally required to obtain goods and services on credit, such as social security numbers, names, and dates of birth. Identity crimes also involve the theft or misuse of an individual's financial identifiers such as credit card numbers, bank account numbers and personal identification numbers.

The methods of identity criminals vary. "Low tech" identity criminals obtain personal and financial identifiers by going through commercial and residential trash, a practice known as "dumpster diving". The theft of wallets, purses and mail is also a widespread practice employed by both individuals and organized groups.

With the proliferation of computers and increased use of the Internet, "high tech" identity criminals began to obtain information from company databases and web sites. In some cases, the information obtained is in the public domain; in others it is proprietary and is obtained by means of a computer intrusion.

The method that may be most difficult to prevent is theft by a collusive employee. Individuals or groups who wish to obtain personal or financial identifiers for a large-scale fraud ring will often pay or extort an employee who has access to this information through his or her employment at a workplace such as a utility billing center, financial institution, medical office or government agency. The collusive employee will access the proprietary data base, copy or download the information, and remove it from the workplace either electronically or simply by walking it out.

Once the criminal has obtained the proprietary information, it can be exploited by creating false "breeder documents" such as a birth certificate or social security card. These documents are then used to obtain genuine, albeit false, identification, such as a driver's license or passport. Now the criminal is ready to use the illegally-obtained personal identification to apply for credit cards or consumer loans or to establish bank accounts. This, in turn, leads to the laundering of stolen or counterfeit checks or to a check-kiting scheme. Our own investigations have frequently involved the targeting of

organized criminal groups that are engaged in financial crimes on both a national and international scale. Many of these groups are prolific in their use of stolen financial and personal identifiers to further their other criminal activity.

Recognizing that the United States Code provided an insufficient deterrent to the commission of identity crimes, Congress recently enacted the Identity Theft Penalty Enhancement Act. This act mandates an additional two-year sentence (or five years, in the case of some offenses) for anyone possessing or using, without lawful authority, a means of identification of another person during and in relation to the commission of numerous other Federal felonies. It is particularly important that this sentence cannot be served as probation or concurrently with any other term of imprisonment.

Agency Coordination

It has been our experience that the criminal groups involved in these types of crimes routinely operate in a multi-jurisdictional environment. This has created challenges for local law enforcement agencies that generally act as the first responders to such criminal activities. By working closely with our federal, state, and local law enforcement partners, as well as international police agencies, we are able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise that bridges jurisdictional boundaries. This partnership approach to law enforcement is exemplified by our financial and electronic crime task forces located throughout the country. These task forces primarily target suspects and organized criminal enterprises engaged in financial and electronic criminal activity that fall within the investigative jurisdiction of the Secret Service.

Members of these task forces, who include representatives from local and state law enforcement, prosecutors' offices, private industry and academia, pool their resources and expertise in a collaborative effort to detect and prevent electronic crimes. The value of this crime fighting and crime prevention model has been recognized by Congress, which has authorized the Secret Service to expand its electronic crime task forces to cities and regions across the country. Recently, four new Electronic Crimes Task Forces (ECTFs) were established in Dallas, Houston, Columbia (SC) and Cleveland, bringing the total number of such task forces to 13.

The Secret Service ECTF program bridges the gap between conventional cyber-crimes investigations and the larger picture of critical infrastructure protection. Secret Service efforts to combat cyber-based assaults that target information and communications systems supporting the financial sector are part of the larger and more comprehensive critical infrastructure protection and counterterrorism strategy.

As part of the Department of Homeland Security, the Secret Service continues to be involved in a collaborative effort targeted at analyzing the potential for financial, identity and electronic crimes to be used in conjunction with terrorist activities. The Secret Service prides itself on an investigative and preventive philosophy that fully involves our partners in the private sector and academia as well as our colleagues at all levels of law

enforcement in combating the myriad types of financial and electronic crimes. Central to our efforts in this arena are our liaison and information exchange relationships with the Bureau of Immigration and Customs Enforcement (ICE), the Department of the Treasury, the Department of State, and the FBI. As Secret Service investigations uncover activities of individuals or groups focusing on doing harm to the United States, appropriate contact is immediately made and information is passed to those agencies whose primary mission is counterterrorism.

As a key element in our strategy of sharing information and cooperating with other agencies involved in the effort to keep America safe, the Secret Service has assigned 58 Special Agents to the FBI's Joint Terrorism Task Forces (JTTFs) and additional personnel to Operation Cornerstone (led by ICE) and the Treasury Department's Financial Crimes Enforcement Network (FinCEN).

The Secret Service currently has 17 permanent foreign offices that support both our protective and investigative missions. Agents in these offices work in cooperation with host country law enforcement officials and contribute to international information sharing and training as well as criminal investigations. The Secret Service also provides training for counterfeit investigations, financial crimes and computer intrusions to our international law enforcement partners.

The Secret Service is actively involved in a number of other government-sponsored initiatives. At the request of the Attorney General, the Secret Service joined an interagency identity theft subcommittee that was established by the Department of Justice (DOJ). This group, which comprises federal, state, and local law enforcement agencies, regulatory agencies, and professional organizations, meets regularly to discuss and coordinate investigative and prosecutorial strategies as well as consumer education programs.

In a joint effort with DOJ, the U.S. Postal Inspection Service, the Federal Trade Commission and the International Association of Chiefs of Police, we are hosting Identity Crime Training Seminars for law enforcement officers. In the last two years we have held seminars for officers in Chicago, Dallas, San Francisco, Las Vegas, Des Moines, Washington D.C., Phoenix, New York, Seattle, San Antonio, Providence, Orlando, Raleigh, Rochester and Denver. These training seminars are focused on providing local and state law enforcement officers with tools and resources that they can immediately put into use in their investigations of identity crime. Additionally, officers are provided resources that they can pass on to members of their community who are victims of identity crime.

Operation Direct Action (ODA) is a task force comprised of the Secret Service and a number of private sector partners. The primary focus of this task force is to target organized criminal groups that are committing large scale financial fraud, specifically credit card "bust out" schemes that may impact our nation's financial infrastructure. A "bust out" scheme is a type of fraud where a criminal obtains multiple credit card accounts and manipulates the lines of credit that are established with each card. The

criminal makes payments with convenience checks issued by another card or with Non-Sufficient Funds (NSF) checks drawn on any number of bank accounts. The criminal is taking advantage of the lag time between the credits to accounts and the issuing banks' determination that the checks were bad.

Preventative Efforts

Another important component of the Secret Service's preventative and investigative efforts is our focus on increasing awareness of issues related to financial crime investigations in general, and of identity crime specifically, both in the law enforcement community and the general public. The Secret Service has tried to educate consumers and provide training to law enforcement personnel through a variety of partnerships and initiatives.

For example, criminals increasingly employ technology as a means of communication, a tool for theft and extortion, and a repository for incriminating information. As a result, the investigation of all types of criminal activity, including identity crime, now routinely involves the seizure and analysis of electronic evidence. In fact, so critical was the need for basic training in this regard that the Secret Service joined forces with the International Association of Chiefs of Police and the National Institute for Justice to create the "Best Practices Guide to Searching and Seizing Electronic Evidence" which is designed for the first responder, line officer and detective alike. This guide assists law enforcement officers in recognizing, protecting, seizing and searching electronic devices in accordance with applicable statutes and policies.

We have also worked with these same partners in producing the interactive, computer-based training program known as "*Forward Edge*," which takes the next step in training officers to conduct electronic crime investigations. *Forward Edge* is a CD-ROM that incorporates virtual reality features as it presents three different investigative scenarios to the trainee. It also provides investigative options and technical support to develop the case. Copies of state computer crime laws for each of the fifty states as well as corresponding sample affidavits are also part of the training program and are immediately accessible for instant implementation.

Thus far, we have distributed over 300,000 "Best Practices Guides" to local and federal law enforcement officers and have distributed, free of charge, over 20,000 *Forward Edge* training CDs.

In addition, we have just completed the Identity Crime Video/CD-ROM which contains over 50 investigative and victim assistance resources that local and state law enforcement officers can use when combating identity crime. This CD-ROM also contains a short identity crime video that can be shown to police officers at their roll call meetings which discusses why identity crime is important, what other departments are doing to combat identity crime, and what tools and resources are available to officers. The Identity Crime CD-ROM is an interactive resource guide that was made in collaboration with the U.S. Postal Inspection Service, the Federal Trade Commission (FTC) and the International

Association of Chiefs of Police. To date, over 40,000 Identity Crime CD-ROMs have been distributed to law enforcement departments and agencies across the United States.

The Secret Service has also assigned a special agent to the FTC as a liaison to support all aspects of that agency's program to encourage the use of the Identity Theft Data Clearinghouse, the nation's central repository for identity theft complaints, as a law enforcement tool. The FTC has done an excellent job of providing people with the information and assistance they need in order to take the steps necessary to correct their credit records, as well as undertaking a variety of "consumer awareness" initiatives regarding identity theft.

It is important to recognize that public education efforts can only go so far in combating the growth of identity crime. Because social security numbers, in conjunction with other personal and financial identifiers, are used for such a wide variety of record keeping and credit related applications, even a consumer who takes appropriate precautions to safeguard such information is not immune from becoming a victim.

Mr. Chairman, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at this time.